Last Time: Solved linear congruence equations using Euclid's Extended Algorithm.

Ex: Solve $12x + 3 \equiv 3x - 5 \mod 17$ for some $x \in \{0, 1, \dots, 16\}$.

Sol: First we manipulate the congruence:

$$12x + 3 \equiv 3x - 5 \mod 17$$

iff $12x - 3x \equiv -5 - 3 \mod 17$

iff $9x \equiv -8 \mod 17$ $\longrightarrow$ $ax \equiv b \mod m$

So now apply Euclid's Algorithm to a, m (i.e. $9, 17$):

$$17 = 9 \cdot 1 + 8 \longrightarrow 8 = 17(1) + 9(-1)$$
$$9 = 8 \cdot 1 + 1 \longrightarrow 1 = 9(1) + 8(-1)$$
$$8 = 1 \cdot 8 + 0$$

Back substitute:

$$\begin{aligned} 1 &= 9(1) + 8(-1) \\ &= 9(1) + (17(1) + 9(-1))(-1) \\ &= 9(1) + 17(-1) - 9(1) \\ &= 9(2) + 17(-1) \end{aligned}$$

Hence $9 \cdot 2 \equiv 1 \mod 17$

i.e. $9^{-1} = 2 \mod 17$

Multiply both sides by the inverse of 9 mod 17:

$x = 1x \equiv 2(9x) \equiv 2(-8) = -16 \equiv 1 \mod 17$

Hence $x = 1$ is the desired solution. ☒

Primes and Prime Factorization

Defn: An $p \in \mathbb{N}$ is *prime* when $p \geq 2$ and if $p = nm$ for some $n, m \in \mathbb{N}$, then either $n = 1$ or $m = 1$.

NB: Equivalently: p is prime when its only positive divisors are 1 and itself, and $p > 1$.

Ex: 2 is prime, 3 is prime, 5 is prime, 7 is prime...

Prop: There are infinitely many primes.

pf: Assume to the contrary there are finitely many primes. Thus we may list the primes in order as $2 \leq p_1 < p_2 < \cdots < p_n$.

Consider the product $Q = p_1 p_2 \cdots p_n + 1$.

(claim: Q is divisible by a prime number not on our list).

(**Lemma (Proof follows this one):** Every natural number $m \geq 2$ is divisible by a prime number.) *

By the lemma, Q is divisible by a prime. Thus $p_k \mid Q$ for some $k \geq 1$ (because our list has all the primes by assumption). Thus we have $Q = p_k m$ for some $m \in \mathbb{Z}$ by defn of div.

Now $$p_k m = Q = p_1 p_2 \cdots p_{k-1} p_k p_{k+1} \cdots p_n + 1$$
$$= p_k (p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n) + 1$$

So $1 = p_k m - p_k (p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n) = p_k (m - p_1 p_2 \cdots p_{k-1} p_{k+1} \cdots p_n)$

Hence $p_k \mid 1$ yields $p_k = 1 \geq 2$ which is absurd.

Thus, we must conclude that there are not finitely many primes; i.e. we've shown the claimed result. ☒

Pf (Lem): (WTS: Every integer $n \geq 2$ is divisible by a prime).

Let $n \in \mathbb{N}$ w/ $n \geq 2$. We proceed by strong induction:

Base Case: If $n = 2$ (or n is any prime), then n is divisible by n, a prime number!

Inductive Step: Suppose the result holds for all $2 \leq k < n$ for some $n \geq 2$. We may assume n is not prime (because we proved the result for n prime as part of our base cases). Because n is not prime, there are integers $m, q \in \mathbb{N}$ such that $n = mq$ and neither m nor q is equal to 1. Hence $1 < m < n$. So m is divisible by a prime number by our Inductive Hypothesis. Thus we obtain $p \mid m$ for some prime p. But $m \mid n$ and we thus have $p \mid n$ by transitivity of divisibility. Hence our inductive step holds.
Thus we may conclude the original statement is true. ☒

Defn: An integer $n > 1$ is composite when it is not prime.

Prop: If n is composite, it has a prime factor at most $\sqrt{n}$.

Pf: Let $n \in \mathbb{N}$ be composite. Assume to the contrary that every prime factor of n is greater than $\sqrt{n}$. Take any such prime factor $p \geq \sqrt{n}$. Thus $n = pk$ for some $k \in \mathbb{N}$. Now $k \leq \sqrt{n}$ (lest $pk > \sqrt{n}\sqrt{n} = n$). Hence Now k has a prime factor $q \leq k \leq \sqrt{n}$. Hence $q \mid k$ and $k \mid n$ yields $q \mid n$, contradicting our assumption. ☒

Consequences: We can compute prime numbers as follows:

Alg (Sieve of Eratosthenes): Given $n \geq 2$, we compute all the primes up to (and possibly including) n as follows:

① List all the integers 1 to n.

② Cross off 1, set $p_1 = 2$.

③ Given a list w/ crossed out numbers and p_i:

Ⓐ Cross off every multiple of p_i (keeping p_i itself).

Ⓑ Find p_{i+1} := the smallest integer which is both greater than p_i and uncrossed.

* Ⓒ If $p_{i+1} > \sqrt{n}$, output the list of uncrossed numbers. Otherwise increment i and repeat from Ⓐ.

Ex: Run Sieve of Eratosthenes on $n = 30$.

NB: $\sqrt{30} < 6$

Sol:

~~1~~	$p_1=2$ 2	$p_2=3$ 3	~~4~~	$p_3=5$ 5	~~6~~	$p_4=7$ 7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

Output: $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ is the set of primes at most 30. ∎

Reason to care about primes: Prime factorization...

Prop (Euclid's Lemma): Let p be a prime number and $a, b \in \mathbb{Z}$. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Remark: We won't prove this here... Proof uses the Well-Ordering Principle.

Prop (Fundamental Theorem of Arithmetic): Given $n \in \mathbb{Z}_+$. There is a unique sequence $p_1 < p_2 < \cdots < p_k$ of primes and a corresponding unique sequence of positive integers $e_1, e_2, \ldots, e_k$ such that $\left[n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} . \right]$ ★

Remark: Often this is stated a little differently:
"n can be factored as a product of prime powers ★ uniquely [up to] the order of the factors".

pf: Proceed by strong induction on n.

Base Case: If $n=1$, then the corresponding sequence of primes is empty (i.e. no primes). Thus we obtain uniqueness. By convention, the empty product is 1, so the result holds in the base case.

Inductive Step: Suppose the result holds for every integer $1 \le k < n$ where $n \ge 2$. Let p be the smallest prime divisor of n (i.e. $p = \min\{q : q \mid n \text{ and } q \text{ is prime}\}$; This set is nonempty by a previous proposition, so well-ordering principle yields that p exists). Now $n = pq$ for some $q \in \mathbb{Z}_+$ by definition of divisibility. Now $1 \le q < n$, so q admits a prime factorization $q = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Hence

$$n = pq = p\, p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$ Now we finish by cases.

If $p = p_1$, the resulting factorization is $n = p_1^{e_1+1} p_2^{e_2} \cdots p_k^{e_k}$.

Otherwise, $p < p_1$ so the resulting factorization is $n = p\, p_1^{e_1} \cdots p_k^{e_k}$.

Sketch for Uniqueness: If factorization wasn't unique, this would contradict uniqueness of q's factorization ... ☑